# Department of Homeland Security
# IAIP Directorate
# Daily Open Source Infrastructure Report
# for 03 September 2004

Current Nationwide Threat Level is
ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS
For info click here
www.whitehouse.gov/homeland

**Daily Overview**

- The Associated Press reports that two airlines that fly from Moscow to the United States have been ordered to tighten security one week after suspected terrorists crashed two Russian planes. (See item 7)
- The Washington Post reports that the Metropolitan Area Transit Authority in Washington, DC, will begin training a select group of commuters this month in ways to evacuate trains and subway tunnels and help fellow passengers during a terrorist attack or rail disaster. (See item 9)
- The New York Times reports more than 30 of the most sensitive and heavily trafficked court buildings in New York State have digital cameras that are linked to a new system that can be monitored from a central location or even from home computers. (See item 24)

**DHS/IAIP Update *Fast Jump***

**Production Industries:** Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
**Service Industries:** Banking and Finance; Transportation; Postal and Shipping
**Sustenance and Health:** Agriculture; Food; Water; Public Health
**Federal and State:** Government; Emergency Services
**IT and Cyber:** Information Technology and Telecommunications; Internet Alert Dashboard
**Other:** Commercial Facilities/Real Estate, Monument &Icons; General; DHS/IAIP Web Information

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated**
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *September 02, Associated Press* — **Crews attempt to restore natural gas service. The southeast South Dakota town of Parkston is without natural gas, and NorthWestern Energy says it appears someone tampered with the equipment and caused the outage.** The company says because the pressure in the lines is down, the gas needs to be turned off at every building in town served by the utility. NorthWestern crews are going door to door to make sure

that happens. Once the gas supply is restored, workers will have to go door to door again to reopen the lines and re−light pilot lights.
Source: http://www.keloland.com/News/NewsDetail4514.cfm?ID=22,34407

2. *September 02, Pennsylvania State University* — **Vulnerability of U.S. power grid identified.** Vulnerabilities inadvertently built into the U.S. power grid, which is one of the most complex systems ever constructed, have been identified by a research team lead by Reka Albert, assistant professor of physics at Pennsylvania State University. **The team's topological analysis of the grid structure reveals that, although the system has been designed to withstand the random loss of generators or substations, its integrity may depend on protecting a few key elements.** "Our analysis indicates that major disruption can result from loss of as few as two percent of the grid's substations," says Albert. One implication of the research is that identification of strategic points in the grid system can enhance defense against interruptions, whether by equipment failure, natural disasters, or human activity. The study, titled "Structural Vulnerability of the North American Power Grid," was published in a recent issue of the journal Physical Review E.
Source: http://www.eurekalert.org/pub_releases/2004−09/ps−vou090204. php

3. *September 01, New Scientist* — **U.S. plans portable nuclear power plants. A nuclear reactor that can meet the energy needs of developing countries without the risk that they will use the by−products to make weapons is being developed by the Department of Energy (DOE).** The aim is to create a sealed reactor that can be delivered to a site, left to generate power for up to 30 years, and retrieved when its fuel is spent. **The developers claim that no one would be able to remove the fissile material from the reactor because its core would be inside a tamper−proof cask protected by a thicket of alarms.** Known as the small, sealed, transportable, autonomous reactor (SSTAR), the machine will generate power without needing refueling or maintenance, says Craig Smith of the DOE's Lawrence Livermore National Laboratory in California. Conventional reactors pose a threat of proliferation because they have to be periodically recharged with fuel, which later has to be removed. Both steps offer operators the chance to divert fissile material to weapons programs as is thought to have happened in North Korea and Iran.
Source: http://www.newscientist.com/news/news.jsp?id=ns99996344

[Return to top]

## Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

## Defense Industrial Base Sector

4. *September 02, Government Computer Week* — **Army urged to step up IT security focus.** The security threat on DoD networks is growing substantially each day, so much so that on two separate occasions this summer, viruses infiltrated two top−secret computer systems at the Army Space and Missile Defense Command. Army Lt. Gen. Larry J. Dodgen, the command's

leader, blamed the viruses, which appeared on the Defense Department's Secret Internet Protocol Router Network, on users and network administrators who were not conducting their jobs in a diligent fashion. Dodgen added that the systems had no virus protection software. He said the incident highlights the need for the DoD to place a "greater emphasis on Defense in depth and risk management principals." **Linton Wells, acting assistant secretary of Defense for Networks and Information Integration, also stressed that network security is one of the biggest issues currently facing the DoD because it impacts everyone −− from the back office to the warfighters on the front lines.** Wells added that the DoD spends $2.2 billion a year on information assurance and is moving in the right direction with the recent unveiling of the first IA architecture to support the Global Information Grid.
Source: http://www.gcn.com/vol1_no1/daily−updates/27138−1.html

5. *September 01, Federal Computer Week* — **Air Force focuses on info.** If hardware and software have been the focus of Air Force information technology efforts in the past, it's information that will drive the future, according to John Gilligan, chief information officer of the Air Force. Gilligan said that idea stems from a simple recognition that information itself is now an enabling capability for the decision−maker and the warfighter. **Getting accurate, timely, complete and usable information to the right person in a secure manner is now the function of IT,** he said. That's going to bring a radical makeover for the Air Force's IT infrastructure. In the past it's been organized around completely separate organizations, each of which had control over its own hardware, software, interfaces and so on, he said. **The future will be one of common interfaces, common data warehouses and a common set of applications delivered as Web−based services.**
Source: http://www.fcw.com/fcw/articles/2004/0830/web−afinfo−09−01−0 4.asp

[Return to top]

## Banking and Finance Sector

6. *September 02, The Record (CA)* — **Man held in laptop theft.** Authorities have arrested a man who allegedly stole a laptop computer containing sensitive information from the home of a Bank of Lodi executive. **San Joaquin County, CA, Sheriff's Office officials said 114 business and individual customers had been notified of the computer's theft from the home of bank Chairman Benjamin Goehring.** John Kevin Dougherty allegedly stole the laptop in addition to credit cards from Goehring's house August 15, Sheriff's Office spokesperson Nelida Stone said. The laptop contained customer loan and taxpayer identification information. **Stone said she didn't know if Goehring was targeted in particular because of his bank position.** Authorities, however, believe Dougherty and others were seeking specific sensitive information such as Social Security and bank account numbers, Stone said.
Source: http://www.recordnet.com/daily/news/articles/090204−gn−3.php

[Return to top]

## Transportation Sector

7. *September 02, Associated Press* — **U.S. tightens security on Russia flights.** Two airlines that fly between Moscow to the United States must check passengers and their carryon bags for bombs, according to a government order Wednesday, September 1, one week after suspected terrorists crashed two Russian planes. **"The U.S. has determined it's prudent to take additional security measures to increase the protection of flights between the U.S. and Russia until we have more information to assess the situation**," said Amy von Walter, a spokesperson for the Transportation Security Administration. The airlines affected are Delta Air Lines and Aeroflot Russian Airlines, which fly to the United States four times a day from Sheremetyevo International Airport. Aeroflot has direct flights from Moscow to New York, Seattle, Los Angeles and Washington, DC, while Delta offers daily flights between Moscow and New York. The two planes that crashed on August 25 after near−simultaneous explosions, killing all 90 people on board, had left Moscow's Domodedovo Airport on domestic flights. The planes belonged to the Russian airline Sibir and a small regional airline, Volga−Aviaexpress. **Delta and Aeroflot were ordered to conduct tests of all passengers and their bags for explosives using various technologies, von Walter said. The airlines also must conduct more thorough screening of all cargo put aboard passenger planes.**
Source: http://newsobserver.com/24hour/nation/story/1619549p−9301709 c.html

8. *September 02, Times Ledger (NY)* — **Port Authority invites ferry plans for airports. The Port Authority of New York and New Jersey has invited ferry companies to submit plans for ferry service linking Lower Manhattan with John F. Kennedy International Airport, LaGuardia Airport and Yonkers. Chairman Anthony Coscia of the Port Authority said in a statement that 40,000 commuters now arrive daily in Manhattan by ferry.** "The use of our waterways has become an important resource as we look to reduce dependence on our bridges, tunnels and existing mass transit systems," Coscia said. The Manhattan−JFK ferry would link a Port Authority dock near Battery Park City and a mooring location near the AirTrain station on Lefferts Boulevard from which JFK users could board the AirTrain for the terminals. Port Authority Executive Director Joseph Seymour said the agency was working on a number of ferry initiatives, including a new five−slip floating terminal under construction at Battery Park City. No specific moorage site was mentioned for LaGuardia, but in the past public boat service has arrived at the Marine Air Terminal.
Source: http://www.timesledger.com/site/news.cfm?newsid=12835318&BRD=2676&PAG=461&dept_id=542415&rfi=6

9. *September 02, Washington Post* — **Metro to prepare riders for terror.** The Metropolitan Area Transit Authority in Washington, DC, will begin training a select group of commuters this month in ways to evacuate trains and subway tunnels and help fellow passengers during a terrorist attack or rail disaster. **Transit officials have developed a highly unusual program that will include walking the volunteer passengers into dark subway tunnels to teach them to navigate live tracks as trains roll by.** The transit system, considered by federal law enforcement to be a prime Washington target for terrorists, said the effort was another step in a campaign to prepare Metro's 1.1 million daily rail and bus riders for catastrophe. "You should be able to be responsible for yourself in an emergency," Metro Transit Police Chief Polly L. Hanson said Wednesday, September 1. "The fact is, there may not be enough first responders, or they might not be able to get to you right away." Hanson said subway tunnels pose particular hazards during an emergency and require specialized training. **The American Public Transportation Association believes the Metro training program is the only one of its kind**

**in the country.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A54436−2004Sep 1.html

[Return to top]

## Postal and Shipping Sector

10. *September 02, Reuters* — **U.S. shuts Malaysia embassy. The U.S. embassy in Malaysia has been shut after the discovery of a "whitish powder" in an envelope sent to the mission, officials say.** "We had an employee open an envelope containing a suspicious substance," U.S. embassy spokesperson Frank Whitaker told Reuters, adding that the embassy was closed around noon, September 2. He gave no more details but Malaysian police said it had been called to the embassy to investigate after the discovery of a "whitish powder" in an envelope that contained no letter and had apparently been posted from the U.S. state of Delaware. In the previous scare, the embassy quarantined some staff after a white powder was found in an envelope which also contained a leaflet purporting to come from a previously unknown group threatening to blow up the embassy and kill Americans in Malaysia unless U.S. troops left Iraq. But the mission remained open during the first scare and fears the powder could be anthrax were eventually disproved by lab tests. "We think it is another scare, but we are taking all precautions," senior assistant police commissioner Aziz Bulat told Reuters. He said the latest powder had been sent for analysis.
Source: http://www.reuters.co.uk/newsPackageArticle.jhtml?type=world News&storyID=575491&section=news

[Return to top]

## Agriculture Sector

11. *September 02, Agence France Presse* — **Foot−and−mouth disease spreads in Zambia.** An outbreak of foot−and−mouth disease that was discovered last week in Zambia's Southern Province has spread to various parts of the country, threatening beef exports, an official said on Thursday, September 2. The disease, which usually kills cattle, is spreading quickly in the Southern African country because of a lack of vaccines. **Agriculture Ministry official Morrison Kunda told state radio that the disease has spread to Central Province where 8,000 animals have been affected and close to 15,000 animals are likely to contract the disease.** Kunda said the government has now banned cattle movement from the Central Province of Zambia, a few days after a similar ban was imposed in Southern Province in an effort to curb the disease.
Source: http://www.mg.co.za/Content/l3.asp?cg=BreakingNews−Africa&ao =121524

12. *September 02, Minot Daily News (ND)* — **Pests to control weed.** A new insect species has been introduced into Ward, ND, in hopes that it will help control one of the state's most noxious weeds. North Dakota Agriculture Commissioner Roger Johnson and Ward County Weed Control Officer Derrill Fick Wednesday, September 1, released 1,000 Canada thistle stem mining weevils in an infested one−acre plot. The larvae bore into the plant and mine toward the main stem, crown, and root, inhibiting the plant's ability to produce seeds and grow roots.

**Johnson added significant reduction of Canada thistle and similar thistle species will result from the weevil's introduction. In several years, stand reductions of 30 to 80 percent will be noted, depending on degree of density of the noxious weed and length of time the weevils have had the opportunity to work.** Johnson said 35 of the 53 counties have signed up for a cooperative agreement to control Canada thistle with the stem mining weevil. According to Johnson, the weevils can be used near water, close to livestock, in pastureland, as well as in traditional or organic cropland.
Source: http://www.minotdailynews.com/news/story/092202004_new2news2 .asp

[Return to top]

## Food Sector

13. *September 02, Associated Press* — **Cargill to enter Brazil pork, poultry industry. U.S. food and farm products conglomerate Cargill Inc. will expand in South America's largest country by paying about $130 million for a controlling stake in one of Brazil's leading poultry and pork producers, Cargill said Wednesday, September 1.** Cargill, one of the world's largest privately owned companies, will buy the 62 percent stake of Seara Alimentos held by Mutual Investments Ltd., a Dutch holding company for U.S. agribusiness giant Bunge Ltd. Brazilian production of meat, chicken, and pork has soared in recent years −− with the chicken business reaping record export profits this year following the bird flu outbreak that hit Asia earlier this year. The Seara deal must be reviewed by Brazilian regulators, but Cargill expects it will close by February. If approved. Seara was founded in 1956 and was one of the Brazil's first chicken exporters. It now sells its products in 70 countries, has nine plants in Brazil and employs 14,500 people. Cargill, with headquarters in Minnetonka, MN, has 101,000 workers in 59 countries and employs about 6,000 people in Brazil, where it has operated for four decades.
Source: http://www.theledger.com/apps/pbcs.dll/article?AID=/20040902/NEWS/409020372/1001/BUSINESS

[Return to top]

## Water Sector

14. *September 02, Fort Detrick Standard* — **Machine offers water testing in field.** More than a dozen researchers gathered at the U.S. Army Center for Environmental Health Research August 25 to see an award−winning water analyzer that cuts in third the time to tell if water is contaminated. Demonstrated by David Putnam, a microbiologist, the machine, called the Coliform Analyzer, meets its early goals of rapidly analyzing bacterial contaminants in water while being simple to operate and smaller and lighter than the normal water analysis set up. **The shoe−box sized machine cuts the weight of conventional analyzers to eight pounds while providing quick answers on whether water is contaminated.** It also incorporates innovations such as replacing a yo−yo−sized filter with one that resembles a dime−sized dreidel and borrowing technology developed by the wine−in−a−box industry for collecting and dispensing water samples. **Further, the machine provides continuous progress reports for up to eight samples, which can be run simultaneously, and gives definitive results in eight**

**hours instead of the 24 hours it normally takes.** The machine can be used to test drinking water, source and surface water, treated water, and recreational areas.
Source: http://www.dcmilitary.com/army/standard/9_18/features/30902−1.html

15. *September 01, American Water Works Association* — **Effluent guidelines for water treatment sector.** The U.S. Environmental Protection Agency (EPA) has announced that it will initiate a rulemaking effort to establish Clean Water Act effluent guidelines for the drinking water supply and treatment industry. In its final biennial effluent guidelines plan for 2004/2005, the agency said it will begin the three−year effort to develop first−ever technology−based regulations for water treatment waste discharges to U.S. waterways. **The EPA said that at the time of the proposal, it had concluded that "almost all of the hazard posed by this industrial sector was due to a few facilities" but that comments suggested guidelines for the sector "because of the potential of drinking water supply and treatment plants to discharge nontrivial amounts of nonconventional and toxic pollutants" such as metals and salts, particularly in sludges and reverse osmosis wastewaters.** The agency estimated that roughly 3,700 water treatment facilities could be subject to such effluent guidelines, which amount to national technology−based standards that are implemented through National Pollutant Discharge Elimination System (NPDES) permits.
Source: http://www.awwa.org/communications/waterweek/

[Return to top]

## Public Health Sector

16. *September 02, Associated Press* — **Virus may have killed two babies. A virus recently discovered in Japan is suspected in two "crib deaths" in Wisconsin −− one in Appleton and the other in Fond du Lac −− raising new questions about how many of these mysterious tragedies might be due to germs.** "This is the first description of this virus in the United States," said Dr. Mark Pallansch, who identified it at the federal Centers for Disease Control and Prevention after a Milwaukee virologist detected it. Whether the virus killed the babies isn't known, although both were sick before they died and had signs of disease in their lungs. Officials are trying to figure out how the novel virus −− human parechovirus−3, or HPEV−3 −− fits in. Japanese scientists published their discovery earlier this year after studying a one−year−old girl who developed a high fever, diarrhea and temporary paralysis in 1999. The virus' origin and how the Wisconsin babies got it are unknown.
Source: http://www.greenbaypressgazette.com/news/archive/local_17624 553.shtml

17. *September 02, New Scientist* — **Cats can spread deadly bird flu.** Cats can catch and spread the bird flu that has ravaged poultry and killed at least 26 people across East Asia in 2004. This is the first time cats have been known to get sick from flu, and means the H5N1 virus has already acquired the ability to spread in some mammals. Thijs Kuiken and colleagues at the Erasmus Medical Centre in Rotterdam, the Netherlands, performed a study after three cats and a zoo leopard living near sick poultry in Thailand were confirmed in February 2004 to have died of H5N1. In the study, cats caught H5N1 by eating infected birds, while two healthy cats housed with the sick animals caught the disease, showing it spreads among cats. **So far the virus seems unable to spread from person to person. If H5N1 acquires this ability, it could cause a lethal pandemic. The World Health Organization fears the virus might do this by**

**hybridising with a human flu in a person infected with both.** What has received less attention, says Kuiken, is the possibility that H5N1 could quietly evolve the ability to spread among humans by itself, by infecting species that select for viruses better adapted to mammals.
Source: http://www.newscientist.com/news/news.jsp?id=ns99996352

[Return to top]

## Government Sector

Nothing to report.
[Return to top]

## Emergency Services Sector

18. *September 02, Denver Post (CO)* — **Emergency drill at DIA.** Denver International Airport (DIA) held its annual disaster drill Wednesday, September 1, staging a plane crash with about 100 victims. DIA shut down a runway for the exercise, which included more than 100 fire and rescue personnel. The drill had heavily made−up volunteers strewn about a donated Boeing 727. **The first rescue and fire fighting crews arrived minutes after the first call, said Denver Fire Department Assistant Chief Buck Wyles, who added that he was troubled that the airport has so few emergency personnel for the first response.**
Source: http://www.denverpost.com/Stories/0,1413,36~53~2374300,00.ht ml

19. *September 02, Jackson Citizen Patriot (MI)* — **Mock crisis involving terrorists, hostages helps officials prepare for the worst.** On Wednesday, September 1, the Jackson County, MI, Airport held a mock terrorism exercise, which involved a plane hijacked by Islamic extremists armed with chemical agents seeking to liberate associates in the state prison complex in Blackman Township. Under a plume of man−made smoke, the make−believe drama culminated with two terrorists surrendering to armed Special Response Team officers in haz−mat suits. Planners crafted a scenario with a Jackson spin by incorporating the state prison and involving Foote Hospital and other agencies like the American Red Cross. **The drill also met requirements of a Department of Homeland Security grant, which was designed to strengthen county first−responder skills dealing with CBRNE (chemical, biohazard, radioactive, nuclear and explosives) situations.** The mock crisis accounted for less than a third of the $60,000 grant.
Source: http://www.mlive.com/news/jacitpat/index.ssf?/base/news−10/1094139301297700.xml

[Return to top]

## Information Technology and Telecommunications Sector

20. *September 02, Secunia* — **Winzip unspecified multiple buffer overflow vulnerabilities.** Multiple buffer overflow and input validation vulnerabilities exist in Winzip 9.0, which potentially can be exploited by a remote user to compromise a user's system. Successful exploitation can potentially lead to execution of arbitrary code. Update to 9.0 SR−1:

http://www.winzip.com/upgrade.htm
Source: http://secunia.com/advisories/12430/

21. *September 02, Computerworld* — **Manhattan presents wireless security challenge for RNC.** IT security researchers have uncovered a significant number of unencrypted wireless devices in close proximity to the Republican National Convention (RNC) at New York's Madison Square Garden. During a two−hour "war drive" around the site of the RNC as well as Manhattan's financial district, security researchers from Newbury Networks Inc. discovered more than 7,000 wireless devices, 1,123 of which were located within blocks of the convention. More important, 67% of those devices were access points that did not have encryption protection. The findings underscore that the huge numbers of open, unsecured wireless networks represent a serious threat to the city's hard−wired infrastructure, said Newbury CEO Michael Maggio. **"A wireless−enabled notebook computer powered up inside Madison Square Garden by a conventioneer or media representative could automatically associate with wireless networks outside of the building**," said Maggio, noting that **such a security gap could allow an attacker to "hop onto" the wired network inside the facility.**
Source: http://www.computerworld.com/mobiletopics/mobile/story/0,108 01,95641,00.html

22. *September 02, SecurityTracker* — **DB2 multiple unspecified vulnerabilities.** Multiple unspecified vulnerabilities exist in DB2 Universal Database, allowing malicious people to compromise a vulnerable system. Two of the vulnerabilities are caused due to boundary errors, which can be exploited by a remote user to execute arbitrary code. There are also some other unspecified errors with an unknown impact. The vendor has issued fixpaks, which address the two buffer overflow vulnerabilities: DB2 8.1: http://www−306.ibm.com/software/data/db2/udb/support/downloa dv8.html and DB2 7.x: http://www−306.ibm.com/software/data/db2/udb/support/downloa dv7.html
Source: http://www.securitytracker.com/alerts/2004/Sep/1011140.html

23. *September 01, The Register* — **PDA security still dismal. Worker apathy about PDA security is putting corporate data in jeopardy.** The storage of the names and addresses of corporate customers on PDAs is now common − but security practices are struggling to keep up with technology usage. Two thirds of users do not use any kind of encryption to protect confidential data on mobile devices, according to a survey commissioned by Pointsec Mobile Technologies and Infosecurity Europe. The Mobile Vulnerability Survey 2004 found that a third of users do not even use password protection on their devices, leaving the information vulnerable to opportunists, hackers or competitors. **The survey findings show that one of the fastest and easiest ways to access corporate data is through unprotected PDAs that are lost or stolen, as they contain business names and addresses, spreadsheets and other corporate documents.** One in eight (13 percent) of respondents to the survey have lost their mobile device.
Source: http://www.theregister.co.uk/2004/09/01/pda_sec/

## Internet Alert Dashboard

**DHS/US−CERT Watch Synopsis**

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**US−CERT Operations Center Synopsis:** The US−CERT Operations Center strongly encourages Windows XP users to upgrade to Service Pack 2 if they have not already done so. SP2 offers significant protection against many of the emergent attacks that target Browser Helper Objects and Cross Domain Vulnerabilities in Internet Explorer. See http://www.us−cert.gov/cas/alerts/SA04−243A.html for more information.

**Current Port Attacks**

| | |
|---|---|
| **Top 10 Target Ports** | 135 (epmap), 137 (netbios−ns), 445 (microsoft−ds), 9898 (dabber), 5554 (sasser−ftp), 1434 (ms−sql−m), 1023 (Reserved), 4899 (radmin), 3127 (mydoom), 1026 (nterm)<br>Source: http://isc.incidents.org/top10.html; Internet Storm Center |

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

# Commercial Facilities/Real Estate, Monument &Icons Sector

24. *September 02, New York Times* — **Court surveillance system. More than 30 of the most sensitive and heavily trafficked court buildings in New York State are bristling with digital cameras that are linked to a new system that can be monitored from a central location or even from home computers.** Who exactly will do the monitoring has yet to be determined, but officials say they hope to expand the technology to even more of the state's roughly 300 court buildings once they are comfortable with the system, which is meant to help them watch out for anything from vandalism to terrorism. Sheng Guo, chief technology officer of the New York State court system, and his team began their project in 2002. They found existing software for integrating camera images both expensive and underpowered, so they built their own system, which in total has cost only about $500,000, including hardware and installation, Guo said. Even as such network−based systems aid in surveillance, they raise the fear that hackers will figure out how to watch the watchers. With the New York system, officials emphasize that the images from courthouses are transmitted over the court system's private high−speed network, not the public Internet.
    Source: http://www.nytimes.com/2004/09/02/technology/circuits/02cour .html

[Return to top]

# General Sector

Nothing to report.

[Return to top]

## DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP Web page (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Alerts − Advisories and Information Bulletins: DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues.

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports.

### DHS/IAIP Daily Open Source Infrastructure Report Contact Information

| | |
|---|---|
| Content and Suggestions: | Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644. |
| Subscription and Distribution Information: | Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information. |

### Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

### DHS/IAIP Disclaimer